TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL

****
IN RE: APPLICATION FOR WARRANT
FOR HISTORICAL CELLSITE
INFORMATION

20 MC 1088
Docket Number

****

SUBMITTED BY: Plaintiff____ Defendant____ DOJ ✓
Name: Andrew Wang
Firm Name: USAO-EDNY
Address: 271 Cadman Plaza East
Brooklyn, New York 11201
Phone Number: 718-254-6311
E-Mail Address: Andrew.Wang2@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES____ NO ✓
If yes, state description of document to be entered on docket sheet:

A) If pursuant to a prior Court Order:
Docket Number of Case in Which Entered:
Judge/Magistrate Judge:
Date Entered:

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

Ongoing criminal investigation; risk of flight and evidence destruction

ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE, AND MAY NOT BE UNSEALED UNLESS ORDERED BY THE COURT.

DATED: Brooklyn, NEW YORK
05/15/2020

U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE 05/15/2020
DATE

MANDATORY CERTIFICATION OF SERVICE:
A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, **B.)** ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation:_____; or **C.)** ✓ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

05/15/2020
DATE

SIGNATURE

WK:ADW
F. #2019R01108

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR DEVICE ASSIGNED CALL NUMBER (347) 249-2432, THAT IS STORED AT PREMISES CONTROLLED BY T-MOBILE US, INC.	**TO BE FILED UNDER SEAL** SEARCH WARRANT APPLICATION FOR HISTORICAL CELL-SITE INFORMATION Case No. 20 MC 1088

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Alexander Turczak, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number (347) 249-2432 ("the SUBJECT PHONE") that is stored at premises controlled by T-Mobile US, Inc. ("T-Mobile"), a wireless telephone service provider with operations at 4 Sylvan Way, Parsippany, New Jersey. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under Title 18, United States Code, Section 2703(c)(1)(A) to require T-Mobile to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since September 2017. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been involved in the investigation of numerous cases involving mail fraud, wire fraud and money laundering. I have also received training on the uses and capabilities of cellular telephones in connection with criminal activity.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy to commit mail fraud and wire fraud) and 1956 (money laundering and conspiracy to commit money laundering) (collectively, the "Subject Offenses") have been committed by Kenneth Ukhuebor. There is also probable cause to search the information described in Attachment A for evidence or instrumentalities of these crimes as further described in Attachment B.

PROBABLE CAUSE

5. Kenneth Ukhuebor is a subject in the government's investigation of an Elder Fraud scheme and an apparently separate Business Email Compromise ("BEC") scheme, both of which appear to have been ongoing since as early as the spring of 2019. Ukhuebor appears to have opened several bank accounts in his own name and the business name Kenbor

Incorporated ("Kenbor Inc.") in order to perpetrate such fraudulent schemes by receiving hundreds of thousands of dollars in proceeds of Elder Fraud and BEC scams.

Kenneth Ukhuebor's Relationship with Kenbor Inc.

6. Kenbor Inc. is a business corporation registered in New York State. Based on New York State Division of Corporations records, Kenbor Inc. was first registered in March 2015 and lists an individual named Patience Osagie as the person who should receive any legal process on behalf of the company. As described below, Kenbor Inc. appears to be either the business operating name or the parent company of a clothing store operating as Kenbor Clothing.

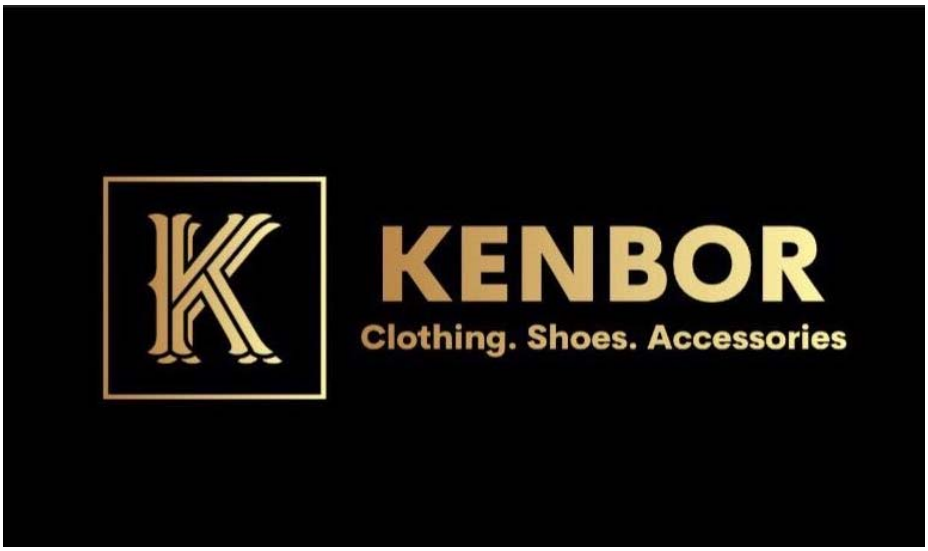
7. On the business social networking website LinkedIn, a search for the name "Patience Osagie" yields five results. Four of those results are for users listed as residing in Nigeria or the United Kingdom. One of the results is for a user listed as residing in the New York area. The Patience Osagie residing in the New York area describes her work experience as being a boutique owner and fashion designer at Kenbor Inc. since January 2015. Notably, this account displays as a profile picture a heavyset adult male with a distinctive beard and wearing sunglasses. As described in more detail below, this individual appears to be Kenneth Ukhuebor.

8. Through my investigation, I have identified two separate accounts on the social networking website Facebook, Inc. ("Facebook") that appear to belong to Kenneth Ukhuebor. The username for one of the accounts is "Kenneth Ukhuebor," and the username for the other account is "Ken Kenbor." Both accounts display profile pictures and other photographs depicting the same heavyset adult male shown in the profile picture for the aforementioned Patience Osagie LinkedIn account.

9. A woman named Precious Ukhuebor appears to be Kenneth Ukhuebor's wife. A Facebook account with the username "Precious Ukhuebor" lists the user as "married." On February 14, 2020, the Precious Ukhuebor Facebook account posted a photo of a woman with the heavyset male believed to be Kenneth Ukhuebor and included a Valentine's Day message. In addition, the same Precious Ukhuebor appears to have an account (username "ukhuebor_precious") on Instagram, a social networking site that allows users to post pictures with captions. Precious Ukhuebor's Instagram page includes numerous photos of Kenneth Ukhuebor with accompanying descriptions that refer to him as her husband.

10. The URL for the Precious Ukhuebor Facebook account is www.facebook.com/patience.osagie.3958.

11. On her Facebook account, Precious Ukhuebor describes her employment as "Kenbor Clothing," using a clickable link that leads to a "Kenbor Clothing" Facebook page. The page describes the business as a "Women's Clothing Store" and includes a post from October 16, 2019 announcing a grand opening. The Kenbor Clothing Facebook page displays the following image as its profile picture:



12. On October 16, 2019, Precious Ukhuebor changed her Facebook profile picture to display the same Kenbor Clothing picture above. Also on October 16, 2019, both the Ken Kenbor and Precious Ukhuebor Facebook users posted links to the Kenbor Clothing Facebook page's grand opening announcement.

13. Records from Facebook reveal that both the Kenbor Clothing and the Ken Kenbor accounts were registered using the same phone number.

14. Based on the foregoing, I believe that Patience Osagie and Precious Ukhuebor are either the same person or close associates of one another. The above information also shows that Kenneth Ukhuebor is married to Precious Ukhuebor and, through his wife, is affiliated with Kenbor Inc.

The Elder Fraud Scheme

15. Elder Fraud schemes often involve fraudsters who target elderly victims by pretending to be the representatives of a foreign national lottery (in which the victim has purportedly won a large sum of money) or a foreign estate (in which the victim has purportedly been named as a beneficiary of the estate and is entitled to a large sum of money). Such schemes sometimes involve promises by fraudsters that the victim will receive a large payment upon the victim's payment to the fraudsters of purported taxes, fees or other invented charges.

16. Persons involved in laundering the proceeds of fraudulent schemes through financial institution accounts, and otherwise, may receive and transfer funds from multiple such schemes at the same time.

17. Among other things, we have have learned through our investigation that in or about the spring of 2019, an unknown person faxed a letter to an 86-year old victim (the "Victim"), the identity of whom is known to me, in New York. The faxed letter stated that the

Victim was entitled to a $26.7 million inheritance following the death of an individual in Spain. The letter directed the Victim to send "taxes" and "fees" related to the inheritance to two Bank of America accounts, one bearing the number XXXXXXXX0762 (the "0762 Account") and the other bearing the number XXXXXXXXX8304 (the "8304 Account"). Bank of America signature cards show that the 0762 Account was opened by and in the name of Kenneth Ukhuebor in March 2013, and that the 8304 Account was opened by Patience Osagie, in April 2015, in the name of Kenbor Inc. In total, the Victim sent more than $200,000 in proceeds to the 0762 Account and the 8304 Account.

The BEC Scheme

18. BEC schemes often involve a computer hacker gaining unauthorized access to a business email account via software, malware or social engineering, blocking or redirecting communications to and/or from the email account, and then using the compromised email account or a separate fraudulent email account (sometimes called a "spoofed" email account)[1] to communicate with unsuspecting personnel from a victim company and trick them into making an unauthorized wire transfer. The fraudster directs the personnel to transmit company funds to the bank account of a third party (sometimes referred to as a "money mule"), which is often a bank account owned, controlled and/or used by individuals involved in the

[1] One way of spoofing an email address is to create an account at a fraudulent domain, where the domain name is altered to appear identical to a real company domain but where it is misspelled by a letter or character. For example, a BEC fraudster might spoof the email address of "John" at "ACME, Inc." (john@acmecompany.com) by creating similar email accounts at a fraudulent domain (e.g., john@acmecornpany.com, replacing the "m" in "company" with the letters "rn," or john@acmecompanies.com). Also, BEC fraudsters sometimes create a fraudulent email account at a legitimate email provider (e.g., john_acmecompany@gmail.com).

scheme. The money may then be laundered by transferring it through numerous bank accounts or by quickly withdrawing it as cash, by check or by cashier's check.

19. The Philadelphia Sign Company ("PSC"), a New Jersey-based sign design, manufacturing and installation company that does business throughout the United States, is one of the victims of the BEC scheme we are investigating. In July 2019, PSC reported to the government that unidentified persons had gained access to PSC's corporate email account and proceeded to send unauthorized emails to numerous PSC clients. For example, Allstate Corporation, a PSC client, wired almost $400,000 to TD Bank account number XXXXXX4749 (the "4749 Account") at the direction of a fraudster sending an unauthorized email that purported to be from PSC.

20. A TD Bank signature card shows that Kenneth Ukhuebor opened the 4749 Account in his own name in April 2013. In addition, TD Bank surveillance camera footage shows that between May 14, 2019 and June 26, 2019, the heavyset man identified as Kenneth Ukhuebor and shown in pictures displayed on (a) the Ken Kenbor Facebook account, (b) the Patience Osagie LinkedIn account, and (c) the Precious Ukhuebor Facebook and Instagram accounts, conducted transactions on the 4749 Account at multiple TD Bank locations.

21. Another victim of the BEC scheme was Meristem Packaging Company LLC ("Meristem"), a packaging company based in Georgia. On or about May 8, 2019, Meristem received two emails from nichole.young@eateryesentials.com, a "spoofed" email account purporting to come from Eatery Essentials, a U.S. company that sells and markets paper and plastic cups and containers. At the direction of the emails sent from the spoofed account, Meristem redirected approximately $72,000 in payments to a TD Bank account number

XXXXXX3439 (the "3439 Account"). TD Bank records show that Patience Osagie opened the 3439 Account in January 2019, in the name of Kenbor Inc.

The Subject Phone's Connection to the Elder Fraud & BEC Schemes

22. Records from Facebook, Inc. reveal that the "Ken Kenbor" Facebook profile is associated with the Yahoo email account kenborpat@yahoo.com.

23. Records from Oath Holdings Inc., Yahoo's parent company, and T-Mobile reveal that a number of the IP addresses through which the kenborpat@yahoo.com account was repeatedly accessed were associated with the SUBJECT PHONE.

24. Records received from TD Bank, Bank of America, Wells Fargo and JPMorgan Chase show that an individual using the name "Alex Osato" currently maintains accounts with each of those banks and provided the SUBJECT PHONE number when opening the accounts. Each of those accounts was opened using a Nigerian passport that appears to be fraudulent, and each of those accounts has been flagged internally by the respective banks as engaging in suspicious activity. "Alex Osato" also provided 2811 Avenue U in Brooklyn, New York 11229 as an address when opening the accounts. This is the same address listed for Kenbor Clothing on its Facebook and several online business listings.

25. Based on these facts, as well as my training, experience and involvement in this investigation, I believe that location data for the SUBJECT PHONE for the period from May 1, 2019 to the present will provide evidence of Kenneth Ukhuebor's and others' involvement in the Subject Offenses. For example, among other things, location data for the SUBJECT PHONE may reveal the presence of Kenneth Ukhuebor or an accomplice at bank locations to access or manage fraudulent proceeds deposited in the 4749 Account or other bank accounts associated with Kenneth Ukhuebor, Precious Ukhuebor, Patience Osagie, Alex Osato,

Kenbor Inc. and others. Other information sought for the SUBJECT PHONE, such as call records and payment information, will provide evidence of the identity of the user of the kenborpat@yahoo.com account and the "Ken Kenbor" Facebook account, and will provide information as to the identity of the person who set up bank accounts receiving the criminal proceeds of the BEC and Elder Fraud schemes described above.

Technical and Other Information

26. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

27. Based on my training and experience, I know that T-Mobile can collect cell-site data about the SUBJECT PHONE. I also know that wireless providers such as T-Mobile typically collect and retain cell-site data pertaining to cellular phones to which they

provide service in their normal course of business in order to use this information for various business-related purposes.

28. Based on my training and experience, I know that T-Mobile also collects per-call measurement data, which T-Mobile also refers to as the "Real-Time Tool" ("RTT"), "Advanced Timing Data" and/or "Per Call Measurement Data" ("PCMD"). RTT, Advanced Timing Data and PCMD data estimates the approximate distance of the cellular device from a cellular tower based on the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

29. Based on my training and experience, I know that wireless providers such as T-Mobile typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as T-Mobile typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT PHONE's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

30. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

31. I further request that the Court direct T-Mobile to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on T-Mobile, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

32. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to any of the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,

Alexander Turczak
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone on May 15, 2020

HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number (347) 249-2432 ("the Account"), that are stored at premises controlled by T-Mobile US, Inc. ("the Provider"), a wireless telephone service provider with operations at 4 Sylvan Way, Parsippany, New Jersey.

ATTACHMENT B

Particular Things to Be Seized

I. Information to Be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under Title 18, United States Code, Section 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period May 1, 2019 to the present:

a. The following information about the customers or subscribers of the Account:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received, as well as per-call measurement data (also known as the "real-time tool" or "RTT" data, "Advanced Timing Data," "Per Call Measurement" data and/or "PCMD").

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence or instrumentalities of violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy to commit mail fraud and wire fraud) and 1956 (money laundering and conspiracy to commit money laundering) involving Kenneth Ukhuebor during the period May 1, 2019 to the present.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government

control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature